

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 5 月 3 0 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 1 5 4 8 7 0
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 1 5 4 8 7 0]

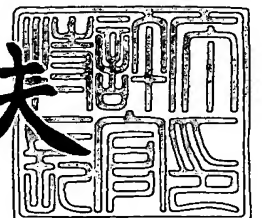
出 願 人 株式会社日立製作所
Applicant(s):

*U.S. Appln. Filed 3-19-04
Inventor: K. Shimooka et al
Matthewly Stanger & Malor
Docket TSM-37*

2 0 0 4 年 3 月 1 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 1 4 9 5 4

【書類名】 特許願

【整理番号】 HK15005000

【提出日】 平成15年 5月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/00

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 下岡 健一

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 浅野 正靖

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100084032

【弁理士】

【氏名又は名称】 三品 岩男

【電話番号】 045(316)3711

【手数料の表示】

【予納台帳番号】 011992

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データの保護装置、方法およびプログラム

【特許請求の範囲】

【請求項 1】

データを記憶するために割り当てられる記憶領域と、前記記憶領域に対してデータの読み込みまたは書き込みを行う計算機と、前記計算機と前記記憶領域との通信を制御する記憶制御装置とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、

イベントの発生を検出するイベント検出部と、

前記イベント検出部がイベントを検出すると、前記計算機と前記記憶領域との通信を停止するよう前記記憶制御装置に対して指示するパス切断部とを有するデータ保護装置。

【請求項 2】

データを記憶するために割り当てられる記憶領域と、前記記憶領域に対してデータの読み込みまたは書き込みを行う計算機と、前記計算機と前記記憶領域との通信を制御する記憶制御装置と、前記計算機に対する不正侵入を検出する不正侵入検出部とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、

前記不正侵入検出部が不正侵入を検出したことを受信するイベント検出部と、

前記イベント検出部が前記不正侵入の検出を受信すると、前記計算機と前記記憶領域との通信を停止するよう前記記憶制御装置に対して指示するパス切断部とを有するデータ保護装置。

【請求項 3】

データを記憶するために割り当てられる記憶領域と、前記記憶領域に対してデータの読み込みまたは書き込みを行う計算機と、前記計算機と前記記憶領域との通信を制御する記憶制御装置と、前記記憶領域内のコンピュータウィルスを検出するコンピュータウィルス検出部とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、

前記コンピュータウィルス検出部がコンピュータウィルスを検出したことを受



信するイベント検出部と、

前記イベント検出部が前記コンピュータウィルスの検出を受信すると、前記計算機と前記記憶領域との通信を停止するよう前記記憶制御装置に対して指示するパス切断部とを有するデータ保護装置。

【請求項 4】

データを記憶するために割り当てられる記憶領域と、前記記憶領域に対してデータの読み込みまたは書き込みを行う計算機と、前記計算機と前記記憶領域との通信を制御する記憶制御装置とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護方法であって、

イベントの発生を検出するステップと、

前記イベントを検出すると、前記計算機と前記記憶領域との通信を停止するよう前記記憶制御装置に対して指示するステップとを有するデータ保護方法。

【請求項 5】

データを記憶するために割り当てられる記憶領域と、前記記憶領域に対してデータの読み込みまたは書き込みを行う計算機と、前記計算機と前記記憶領域との通信を制御する記憶制御装置とを有する計算機システムに対して、前記記憶領域のデータ保護を情報処理装置に実行させるプログラムであって、

イベントの発生を検出する処理と、

前記イベントを検出した後、前記計算機と前記記憶領域との通信を停止するよう、前記記憶制御装置に対して指示する処理とを前記情報処理装置に実行させるプログラム。

【請求項 6】

データを記憶するために割り当てられる記憶領域と、前記記憶領域に対してデータの読み込みまたは書き込みを行う計算機と、前記計算機と前記記憶領域との通信を制御する記憶制御装置と、前記記憶領域のデータを保護するデータ保護装置とを有する計算機システムであって、

前記データ保護装置は、

イベントの発生を検出するイベント検出部と、

前記イベント検出部がイベントを検出すると、前記計算機と前記記憶領域との

通信を停止するよう前記記憶制御装置に対して指示するパス切断部とを有する計算機システム。

【請求項 7】

データを記憶するために割り当てられる記憶領域と、前記記憶領域の複製データを記憶するために割り当てられる複製領域と、前記記憶領域から前記複製領域へのデータ転送を制御する記憶制御装置とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、

イベントの発生を検出するイベント検出部と、

前記イベント検出部がイベントを検出すると、前記記憶領域から前記複製領域へのデータ転送を停止するよう前記記憶制御装置に対して指示する複製停止部とを有するデータ保護装置。

【請求項 8】

データを記憶するために割り当てられる記憶領域と、前記記憶領域の複製データを記憶するために割り当てられる複製領域と、前記記憶領域に対してデータの読み込みまたは書き込みを行う計算機と、前記記憶領域から前記複製領域へのデータ転送を制御する記憶制御装置と、前記計算機に対する不正侵入を検出する不正侵入検出部とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、

前記不正侵入検出部が不正侵入を検出したことを受信するイベント検出部と、

前記イベント検出部が前記不正侵入の検出を受信すると、前記記憶領域から前記複製領域へのデータ転送を停止するよう前記記憶制御装置に対して指示する複製停止部とを有するデータ保護装置。

【請求項 9】

データを記憶するために割り当てられる記憶領域と、前記記憶領域の複製データを記憶するために割り当てられる複製領域と、前記記憶領域から前記複製領域へのデータ転送を制御する記憶制御装置と、前記記憶領域内のコンピュータウィルスを検出するコンピュータウィルス検出部とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、

前記コンピュータウィルス検出部がコンピュータウィルスを検出したことを受

信するイベント検出部と、

前記イベント検出部が前記コンピュータウィルスの検出を受信すると、前記記憶領域から前記複製領域へのデータ転送を停止するよう前記記憶制御装置に対して指示する複製停止部とを有するデータ保護装置。

【請求項 10】

データを記憶するために割り当てられる記憶領域と、前記記憶領域の複製データを記憶するために割り当てられる複製領域と、前記記憶領域から前記複製領域へのデータ転送を制御する記憶制御装置とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護方法であって、

イベントの発生を検出するステップと、

前記イベントを検出すると、前記記憶領域から前記複製領域へのデータ転送を停止するよう前記記憶制御装置に対して指示するステップとを有するデータ保護方法。

【請求項 11】

データを記憶するために割り当てられる記憶領域と、前記記憶領域の複製データを記憶するために割り当てられる複製領域と、前記記憶領域から前記複製領域へのデータ転送を制御する記憶制御装置とを有する計算機システムに対して、前記記憶領域のデータ保護を情報処理装置に実行させるプログラムであって、

イベントの発生を検出する処理と、

前記イベントを検出すると、前記記憶領域から前記複製領域へのデータ転送を停止するよう前記記憶制御装置に対して指示する処理とを前記情報処理装置に実行させるプログラム。

【請求項 12】

請求項 5 または 11 に記載したプログラムを記録した情報処理装置読み取り可能な記憶媒体。

【請求項 13】

データを記憶するために割り当てられる記憶領域と、前記記憶領域の複製データを記憶するために割り当てられる複製領域と、前記記憶領域から前記複製領域へのデータ転送を制御する記憶制御装置と、前記記憶領域のデータを保護するデ

ータ保護装置とを有する計算機システムであって、

前記データ保護装置は、

イベントの発生を検出するイベント検出部と、

前記イベント検出部がイベントを検出すると、前記記憶領域から前記複製領域へのデータ転送を停止するよう前記記憶制御装置に対して指示する複製停止部とを有する計算機システム。

【請求項 14】

請求項 13 記載の計算機システムであって、

前記記憶制御装置は、

前記記憶領域への書込みデータを、一定時間遅らせて、前記複製領域へ転送する計算機システム。

【請求項 15】

請求項 13 記載の計算機システムであって、

前記複製領域は複数設けられ、

前記記憶制御装置は、

前記記憶領域への書込みデータを転送する対象を、一定時間毎に、前記複数の複製領域間で切り替える計算機システム。

【請求項 16】

請求項 15 記載の計算機システムであって、

前記複数の複製領域の所定のデータを読込み、それぞれの所定のデータ間の差異を検出する改竄検知部をさらに有し、

前記イベント検知部が検出するイベントは、前記改竄検知部からの所定のデータ間の差異の検出結果である計算機システム。

【請求項 17】

請求項 16 記載の計算機システムであって、

前記記憶領域に対してデータの読込みまたは書込みを行う計算機をさらに有し、

前記記憶制御装置は、さらに前記計算機と前記記憶領域との通信を制御し、

前記データ保護装置は、前記イベント検知部が前記イベントを検出すると、前

記計算機と前記記憶領域との通信を停止するよう前記記憶制御装置に対して指示する計算機システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、計算機システムに対する不正行為を検出した場合に、計算機システムのデータを保護する技術に関する。

【0002】

【従来の技術】

近年、コンピュータネットワークの普及に伴い、計算機システムを利用した電子商取引などのサービス事業が活発に行なわれるようになっている。一方で、計算機システムに対する不正侵入、コンピュータウィルス等（以下、これらを総称して「不正行為」とする）によるデータ破壊、データ漏洩、データ改竄などの被害が深刻な問題となっている。これらの不正行為によるデータ破壊等は、計算機システムが保持する取引情報などを失わせ、莫大な損失を発生させるおそれがある。これにより、当該計算機システムの運営企業に対する信頼も失墜させかねない。また、破壊等されたデータを復旧するためには、一般に、相当の費用と時間とが必要となる。このため、計算機システムにおいて、不正行為からデータを保護することは、極めて重要である。

【0003】

不正行為への対策としては、まず第1に防止が挙げられる。従来から、計算機システムと外部ネットワークとの間におけるファイアウォールの構築、ワンタイムパスワードなどによるユーザ認証、ユーザ毎にアクセス可能なファイル・プログラムを定義するACL（Access Control List）の設定等により、計算機システムへの不正行為を阻止することが行なわれてきた。しかし、不正行為の手法は日々進化、多様化しており、完全に防止することは事実上不可能に近い。

【0004】

そこで、防止できずに侵入された場合に備えて、監視および事後対応が重要と

なる。従来から知られている代表的な監視手段としては、不正侵入に対する侵入検知システム（IDS：Intrusion Detection System）、コンピュータウイルスに対するウイルス検知ソフトウェアが挙げられる。

【0005】

侵入検知システムは、例えば、ログファイルのモニタやポートスキャンの解析を行なって不正侵入等を監視する。そして、不正侵入等を検知した場合には、侵入者とのセッションを切断したり、侵入された計算機システムと外部ネットワークとの間にあるフロントエンドのスイッチを操作して侵入元とのパスを切断したりする。また、ウイルス検知ソフトウェアは、例えば、ファイルの内容とコンピュータウイルスのコードパターンとのマッチングを行なうことによりコンピュータウイルスの検査を行なう。そして、コンピュータウイルスを検知した場合には、感染したファイルを削除したり、ウイルスパターンを消去したりする。これらの技術の詳細については、例えば、非特許文献1に記載されている。

【0006】

【非特許文献1】

財団法人マルチメディア振興センターネットワーク管理部会、“初心者でも分かるネットワーク管理入門”、6. 3. 3. 侵入検知システム、[online]、平成14年5月15日、[平成14年12月19日検索]、インターネット<URL：<http://www.fmmc.or.jp/~fm/nwmg/manage/main.html>>

【0007】

【発明が解決しようとする課題】

一般に、侵入検知システムは、不正侵入が行なわれてから不正侵入を検出するまでに、ある程度の時間を必要とする。侵入者はこの時間を利用し、侵入先の計算機システムにトロイの木馬を仕掛けたり、再侵入のためのバックドア（裏口）を設けたりすることがある。ここでトロイの木馬とは、無害だと思って実行すると破壊活動を起こしたり、コンピュータウイルスを感染させたりする偽装したプログラムである。

【0008】

この場合、上述のセッションの切断あるいはフロントエンドのパス切断では、

計算機システム内のデータを十分には保護できない。なぜなら、正規ユーザがトロイの木馬をそれと知らず起動してしまったり、侵入者がバックドアから侵入検知システムをすり抜け、再侵入できてしまう可能性があるからである。

【0009】

また、他のファイルやプログラムに次々と感染していく自己増殖型のコンピュータウイルスに感染した場合には、ウイルス検知ソフトウェアがコンピュータウイルスを検出し削除したとしても、他のファイル等を検査するまでに感染が広がってしまう可能性がある。

【0010】

そこで、本発明は、計算機システムに対する不正行為を検出した場合に、計算機システムのデータを保護することを目的とする。

【0011】

【課題を解決するための手段】

上記目的を達成するため、本発明の第1の態様であるデータ保護装置は、データを記憶するために割り当てられる記憶領域と、前記記憶領域に対してデータの読み込みまたは書き込みを行う計算機と、前記計算機と前記記憶領域との通信を制御する記憶制御装置とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、イベントの発生を検出するイベント検出部と、前記イベント検出部がイベントを検出すると、前記計算機と前記記憶領域との通信を停止するよう前記記憶制御装置に対して指示するパス切断部とを有する。

【0012】

発生を検出するイベントとしては、侵入検知部あるいはウイルス検知部の不正行為検出とすることができる。

【0013】

本態様によれば、不正行為を検出した際、不正行為を受けた計算機とその記憶領域の間のバックエンドのパスを切断することにより、データを保護することができる。

【0014】

また、上記目的を達成するため、本発明の第1の態様であるデータ保護装置は

、データを記憶するために割り当てられる記憶領域と、前記記憶領域の複製データを記憶するために割り当てられる複製領域と、前記記憶領域から前記複製領域へのデータ転送を制御する記憶制御装置とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、イベントの発生を検出するイベント検出部と、前記イベント検出部がイベントを検出すると、前記記憶領域から前記複製領域へのデータ転送を停止するよう、前記記憶制御装置に対して指示する複製停止部とを有する。

【0015】

記憶制御装置は、前記記憶領域への書込みデータを、一定時間遅らせて、前記複製領域へ転送したり、複製領域を複数設けて、記憶領域への書込みデータを転送する対象を、一定時間毎に、前記複数の複製領域間で切り替えることができる。

【0016】

本態様によれば、さらに、不正行為が行なわれる前のデータの複製を確保することができる。

【0017】

【発明の実施の形態】

＜第1の実施形態＞

図1は第1の実施形態のシステム構成を示したブロック図である。

【0018】

第1の実施形態のシステムは、フロントエンドのスイッチ30と、ホスト40と、バックエンドのスイッチ50と、記憶装置60と、データ保護装置70とを有し、ネットワーク20に接続している。

【0019】

尚、データ保護装置70は、本実施形態並びに他の実施形態においても1個の独立した装置として記載しているが、ホスト40内部に設けてもよいし、スイッチ30内部に組み込んでもよい。また、スイッチ50も、本実施形態並びに他の実施形態においても1個の独立した装置として記載しているが、ホスト40内部に設けてもよいし、記憶装置60内部に設けてもよい。また、記憶装置60も、

本実施形態並びに他の実施形態においても 1 個の独立した装置として記載しているが、ホスト 4 0 内部に設けてもよい。更に、ホスト 4 0 とデータ保護装置 7 0 との関係は、図 1 並びに他の図においても 1 対 1 の関係で記載しているが、多対 1 であってもよい。また、ホスト 4 0 と記憶装置 6 0 との関係も、図 1 において 1 対 1 で記載しているが、1 対多、多対 1、あるいは、多対多であってもよい。

【0 0 2 0】

ネットワーク 2 0 に接続した計算機 1 0 は、ホスト 4 0 が提供するサービスを利用するための端末として用いられる。しかし、クラッカーが計算機 1 0 を用いてホスト 4 0 に対する不正行為を行うこともあり得る。計算機 1 0 としては、例えば PC (Personal Computer) や携帯情報端末などがある。尚、計算機 1 0 は、図 1 並びに他の図においても 1 台しか記載していないが、複数台存在していてもよい。

【0 0 2 1】

ネットワーク 2 0 は、例えば、IP (Internet Protocol) を用いた Internet、LAN (Local Area Network)、WAN (Wide Area Network)、あるいは、FC (Fibre Channel) を用いた SAN (Storage Area Network) 等で構成することができる。

【0 0 2 2】

フロントエンドのスイッチ 3 0 は、ネットワーク 2 0 とホスト 4 0 との接続を制御する。尚、本実施形態並びに他の実施形態においても、スイッチ 3 0 が存在せず、ネットワーク 2 0 とホスト 4 0 とが直結していてもよい。

【0 0 2 3】

ホスト 4 0 は、スイッチ 3 0、ネットワーク 2 0 を介して計算機 1 0 に電子商取引や動画像ストリーミングなどのサービスを提供する。ただし、ホスト 4 0 は、サービス提供用ホストには限られず、例えば、外部にサービスを行なわない内部データ管理用ホストであってもよい。ホスト 4 0 は、フロントエンドのスイッチ 3 0 とのインタフェースであるポート 4 1 と、不正アクセスを検出するための侵入検知プログラム 4 3 およびコンピュータウィルスを検出するためのウィルス

検知ソフトウェア 44 を格納した記憶領域 42 と、メモリ 45 と、プロセッサ 46 と、バックエンドのスイッチ 50 とのインタフェースであるポート 47 と、データ保護装置 70 とのインタフェースであるポート 48 とを備えて構成される。

【0024】

なお、侵入検知プログラム 43、ウィルス検知ソフトウェア 44 等は、本実施形態並びに他の実施形態においてもホスト 40 が備える記憶領域 42 に格納されているよう記載しているが、記憶装置 60、データ保護装置 70、他の計算機内の記憶領域、あるいは記憶媒体に格納されていてもよい。これらの場合、ホスト 40 は記憶領域 42 を省いて構成してもよい。また、侵入検知プログラム 43 およびウィルス検知ソフトウェア 44 は双方存在することが好ましいが、いずれか一方のみであってもよい。また、ポート 41、47 は、図 1 並びに他の図においてもそれぞれ 1 個ずつ記載しているが、それぞれ複数存在していてもよい。

【0025】

記憶装置 60 は、保護すべきデータを格納する記憶領域 64 を備えた記憶装置である。記憶領域 64 には、例えば、計算機 10 に提供するサービスを実行するためのプログラム、その他のデータを格納する。また、記憶装置 60 は、データをやり取りするスイッチ 50 とのインタフェースであるポート 61 と、構成情報の取得や設定を行うインタフェースである SVP (Service Processor) 62 と、SVP 62 で設定された構成情報に基づいてポート 61 と記憶領域 64 との接続を制御するコントローラ 63 とを備えている。尚、ポート 61 および記憶領域 64 は、図 1 では 1 個ずつ記載しているが、それぞれ複数個存在してもよい。

【0026】

データ保護装置 70 は、本発明の特徴的な装置であり、ホスト 40 とのインタフェースであるポート 71 と、記憶領域 72 と、メモリ 75 と、プロセッサ 76 とを備えている。記憶領域 72 は、後述する侵入検知部 43 x およびウィルス検知部 44 x の不正行為検出結果を受信するための不正行為受信プログラム 73 とホスト 40 とホスト 40 が利用している記憶領域 64 とのパスを切断する処理を行なうためのデータ保護プログラム 74 とを格納している。なお、不正行為受信

プログラム 73 およびデータ保護プログラム 74 は、他の計算機や記憶装置あるいは記憶媒体に格納されていてもよい。この場合、記憶領域 72 は省くことができる。なお、データ保護装置 70 は、専用装置として構成するほか、PC 等の一般的な情報処理装置等で構成することができる。

【0027】

次に、本実施形態のシステムにおける動作を説明する。

【0028】

ホスト 40 は、提供するサービスのプログラムをメモリ 45 にロードし、プロセッサ 46 により実行する。前記プログラムは、計算機 10 からの要求によって、または定期的に、または、あるイベントの発生を契機として、ポート 47、バックエンドのスイッチ 50、記憶装置 60 のポート 61、コントローラ 63 を介し、記憶領域 64 のデータを読み書きし、ポート 41、フロントエンドのスイッチ 30、ネットワーク 20 を介し、計算機 10 にサービスを提供する。

【0029】

同時に、侵入検知プログラム 43、ウイルス検知ソフトウェア 44 も、メモリ 45 にロードされ、プロセッサ 46 により実行される。これにより、ホスト 40 に侵入検知部 43x、ウイルス検知部 44x（いずれも図示せず）が仮想的に構成され、これらが不正行為等がホスト 40 に対して行われていないかを監視する。尚、侵入検知プログラム 43、ウイルス検知ソフトウェア 44 は、データ保護装置 70 あるいはその他の計算機内のメモリにロードされ、ネットワーク経由でホスト 40 を監視するようにしてもよい。

【0030】

また、データ保護装置 70 における不正行為受信プログラム 73 も、メモリ 75 にロードされ、プロセッサ 76 により実行される。これにより、データ保護装置 70 に不正行為受信部 73x（図示せず）が仮想的に構成され、不正行為検出の通知を待ち受ける。なお、不正行為受信部 73x は、侵入検知部 43x あるいはウイルス検知部 44x が不正行為を検出したかどうかを能動的に監視するようにしてもよい。この場合、データ保護装置 70 自身のセキュリティのため、データ保護装置 70 から他装置へのアクセスは許可するが、ホスト 40 などの他装置

からデータ保護装置 70 へのアクセスは許可しないよう設定することが好ましい。
。

【0031】

図 2 は、本実施形態のシステムにおいてホスト 40 が不正行為を受けてから記憶領域 64 のデータを保護するまでの流れを示すシーケンス図である。

【0032】

クラッカー（侵入者）が計算機 10 を用いてホスト 40 に不正侵入したり、コンピュータウイルスを送り込んだとする（S101）。

【0033】

侵入検知部 43x がホスト 40 に対する不正侵入を検出する（S103）と、不正行為受信部 73x にポート 48、71 を介して通知する（S104）。また同様に、ウイルス検知部 44x がコンピュータウイルスを検出すると、ポート 48、71 を介して不正行為受信部 73x に通知する。

【0034】

不正行為受信部 73x は、ホスト 40 に対する不正行為の検出を受信すると、データ保護プログラム 74 をメモリ 75 にロードし、プロセッサ 76 に実行させる（S105）。これにより、データ保護装置 70 に、データ保護部 74x（図示せず）が仮想的に構成される。尚、データ保護プログラム 74 は、あらかじめメモリ 75 にロードしておいてもよい。

【0035】

データ保護部 74x は、ホスト 40 と記憶領域 64 との間のバックエンドのパスを切断するような構成変更を、ポート 71 を介して、スイッチ 50 あるいは SVP62 に対して命令する（S106）。

【0036】

これにより、侵入検知部 43x が不正侵入を検出する前に、トロイの木馬が記憶領域 64 等に仕込まれた場合であっても、ホスト 40 と記憶領域 64 との間のバックエンドのパスが切断されるため、トロイの木馬が記憶領域 64 のデータ改竄を試みても（S107）、ホスト 40 から記憶領域 64 へアクセスすることができず失敗する（S108）。

【0037】

このように本実施形態によれば、不正侵入の事後的に引き起こされる可能性があるデータ破壊等を防止することができる。

【0038】

また、侵入検知部 43x が不正侵入を検出する前に、侵入者が再侵入のためのバックドアを仕掛けたとしても、再侵入の際には、ホスト 40 と記憶領域 64 との間のバックエンドのパスが切断されているため、やはり記憶領域 64 のデータにアクセスすることはできない。

【0039】

記憶領域 64 に自己増殖型コンピュータウイルスが仕掛けられた場合には、ウイルス検知部 44x がコンピュータウイルスを検出した時点には、別ファイルに感染している可能性がある。しかし、データ保護プログラム 74 がホスト 40 と記憶領域 64 との間のパスを切断するため、前記感染ファイルがメモリ 45 にロードされ実行される（発病する）ことがない。すなわち、更なる感染（破壊）から記憶領域 64 のデータを保護することができる。

【0040】

次に、S106におけるバックエンドのパスを切断する方法について説明する。本発明はバックエンドのパスを切断する方法については限定しないが、例えば、スイッチ 50 のゾーニングを利用する方法、記憶装置 60 のパス構成管理を利用する方法、記憶装置 60 のACLを利用する方法がある。データ保護部 74x はこれらのいずれか 1 つを実行してもよいし、複数を組み合わせて実行してもよい。

【0041】

まず、スイッチ 50 のゾーニングを利用する方法を説明する。ゾーニングとは、スイッチにおいて特定のポート間でのみ通信を許す機能である。例えば、ゾーンをポート a、b、c で構成すると、スイッチは、ポート b がポート a、c とは通信できるが、ポート d とは通信できないように制御する。

【0042】

図 3 は、本実施形態におけるスイッチ 50 が保持するゾーニングテーブル 10

0 の一例を示す図である。

【 0 0 4 3 】

ゾーン I D 1 0 1 は、スイッチ 5 0 内でゾーンを一意に識別する値である。尚、図 3 ではゾーン I D 1 0 1 を数字で記載しているが、文字列であってもよい。

【 0 0 4 4 】

ポート I D リスト 1 0 2 は、ゾーンを構成する各ポートのポート I D のリストである。前記ポート I D はポートを一意に識別するための値である。ポート I D としては、例えばポート名称や WWN (W o r l d W i d e N a m e) などがある。

【 0 0 4 5 】

データ保護部 7 4 x は、ポート 7 1 を介し、スイッチ 5 0 に対してゾーニングテーブル 1 0 0 の全ポート I D リスト 1 0 2 からポート 4 7 を削除するよう命令する。ここでポート I D リスト 1 0 2 の構成ポートが 1 個になった場合は、当該ゾーン全体を削除してもよい。

【 0 0 4 6 】

例えばポート 4 7 をポート a とすると、図 3 の例では、データ保護部 7 4 x により、ゾーン I D 1 がポート b、c でのみ構成されるようになる。

【 0 0 4 7 】

この結果ポート 4 7 はどの記憶装置 6 0 にもアクセスできなくなり、ゆえに記憶領域 6 4 内のデータを保護できる。

【 0 0 4 8 】

つぎに、バックエンドのパスを切断する方法として、記憶装置 6 0 のパス構成管理を利用する方法を説明する。

【 0 0 4 9 】

パス構成管理とは、ホスト側から見た記憶領域の I D と記憶装置内部での記憶領域の I D の対応付けを管理する機能である。前記対応付けがなされていない記憶領域へはホストからアクセスできない。

【 0 0 5 0 】

図 4 は、本実施形態におけるコントローラ 6 3 が保持するパス構成テーブル 1

10 の一例を示す図である。

【0051】

内部ポート ID 111 は記憶装置 60 内のポート 61 を一意に識別するための ID である。ホスト LUN (Logical Unit Number) 112 は、ホスト 40 側から見た記憶領域 64 の ID である。内部 LUN 113 は、記憶装置 60 内において記憶領域 64 を一意に識別する ID である。

【0052】

図 4 の例では、ホスト 40 がポート A を介して 1 番の記憶領域にアクセスを試みると、内部 LUN が 156 である記憶領域 64 にアクセスすることになる。

【0053】

尚、ホスト LUN 112、内部 LUN 113 は、図 4 ではそれぞれ数字で記載しているが、文字列であってもよい。

【0054】

データ保護部 74x は、ポート 71、SVP 62 を介し、コントローラ 63 に対して、パス構成テーブル 110 からホスト 40 が利用する記憶領域 64 に該当する項目を削除するよう命令する。ここで、該当する項目を判別するために、侵入検知部 43x またはウィルス検知部 44x は不正行為の検出を不正行為受信部 73x に通知する際に、ホスト 40 が利用しているポート 61 の内部ポート ID 111 と記憶領域 64 のホスト LUN 112 の情報を同時に送信する。データ保護部 74x は不正行為受信部 73x から前記情報を受け取り、パス構成テーブル 110 から前記情報に該当する項目を削除するようコントローラ 63 に要求する。尚、ホスト 40 が利用する記憶領域 64 が運用時に不変であるならば、本実施形態におけるシステムの管理者が予めデータ保護部 74x に対してホスト 40 と記憶領域 64 の内部 LUN 113 の情報を与えておいてもよい。前記情報の設定は、データ保護装置 70 が有するキーボードやマウスなどの入力装置を用い、データ保護部 74x が提供する UI (User Interface) を通じて実行する。この場合、不正行為受信部 73x がホスト 40 に対する不正行為検出を受信すると、データ保護部 74x は前記情報を用い、パス構成テーブル 110 から前記記憶領域 64 の内部 LUN 113 に該当する項目をすべて削除するようコ

ントローラ 63 に要求する。

【0055】

例えばホスト 40 が利用する記憶領域 64 の内部 LUN 113 を 156 とすると、図 4 の例では、データ保護部 74x により第 1 行と第 4 行の項目が削除される。

【0056】

この結果、記憶領域 64 はどのホスト 40 からアクセスされなくなる。これにより、記憶領域 64 内のデータは保護される。

【0057】

つぎに、バックエンドのパスを切断する方法として、記憶装置 60 の ACL を利用する方法を説明する。

【0058】

記憶装置の ACL とは、各記憶領域に対して特定のホスト側のポートからしかアクセスを受け付けない機能である。

【0059】

図 5 は、本実施形態におけるコントローラ 63 が保持する ACL テーブル 120 の一例を示す図である。

【0060】

内部ポート ID 121 は記憶装置 60 内のポート 61 を一意に識別するための ID である。ホスト LUN 122 は、ホスト 40 側から見た記憶領域 64 の ID である。尚、ホスト LUN の代わりに、記憶装置 60 内において記憶領域 64 を一意に識別する ID である内部 LUN を用いてもよい。ホストポート ID リスト 123 は、内部ポート ID 121 とホスト LUN 122 で表されるパスを利用できるポート 47 のポート ID のリストである。即ち、図 4、5 の例の場合、ホスト側のポート a、b、c は記憶装置側のポート A を介して内部 LUN が 156 である記憶領域 64 にアクセスできるが、ポート d、e はアクセスできない。

【0061】

データ保護部 74x は、ポート 71、SVP 62 を介し、コントローラ 63 に対して ACL テーブル 120 内のすべてのホストポート ID リスト 123 からポ

ート 47 を削除するよう命令する。ここでホストポート ID リスト 123 の構成ポートがなくなった場合、その項目自身を削除してもよい。

【0062】

例えば、ポート 47 をポート a とすると、図 5 の例では、データ保護部 74x により第 1 行と第 2 行とからポート a が削除される。

【0063】

この結果ポート 47 はどの記憶領域 64 にもアクセスできなくなる。これにより記憶領域 64 内のデータを保護できる。

【0064】

「スイッチ 50 のゾーニングを利用する方法」と「記憶装置 60 の ACL を利用する方法」とは同等の効果があるが、「記憶装置 60 のパス構成管理を利用する方法」は少し効果が異なる。前者の 2 方法は不正行為を受けたホスト 40 からのみ記憶領域 64 へアクセスできなくなるのに対し、後者の方法はすべてのホストから記憶領域 64 へアクセスできなくなる。すなわち、前者の方法を用いると、不正行為を受けていないホストは継続して記憶領域 64 へアクセスでき、サービスを提供し続けられる。よって、データ保護部 74x は、記憶領域 64 を複数のホストで共有している場合であって、記憶領域 64 のデータを改竄されていたりコンピュータウイルスが侵入していないことが明らかな場合には前者の方法を採用し、そうでない場合は後者の方法を採用することが好ましい。

【0065】

以上のように、本実施形態では侵入検知部 43x またはウイルス検知部 44x が不正行為を検出すると、データ保護部 74x がホスト 40 と記憶領域 64 との間のバックエンドのパスを切断する。これにより、侵入検知部 43x あるいはウイルス検知部 44x が不正行為を検出する前に、トロイの木馬あるいはバックドアを仕掛けられたり、コンピュータウイルスに感染したとしても、記憶領域 64 のデータを保護できる。ホスト 40 からデータを取得しようとしても記憶領域 64 へアクセスできないし、逆に記憶領域 64 に存在するコンピュータウイルスが、メモリ 45 にロードされプロセッサ 46 により実行されることがないためである。

＜第2の実施形態＞

図6は、第2の実施形態のシステム構成を示したブロック図である。

【0066】

第2の実施形態のシステムは、フロントエンドのスイッチ30と、ホスト40と、バックエンドのスイッチ50と、記憶装置60a、60bと、データ保護装置70とを有し、ネットワーク20に接続している。また、ネットワークには計算機10が接続している。

【0067】

計算機10と、ネットワーク20と、フロントエンドのスイッチ30と、ホスト40と、バックエンドのスイッチ50とは、第1の実施形態と構成、機能とも同様とすることができる。

【0068】

記憶装置60aは、第1の実施形態の記憶装置60に加え、記憶装置60bとのインタフェースであるポート65aと、記憶領域64から複製領域67へのデータ反映を一定時間遅らせる転送遅延部66とを更に有する。

【0069】

記憶装置60bは、第1の実施形態の記憶装置60に加え、記憶装置60aとのインタフェースであるポート65bと、記憶領域64の複製データを保持する記憶領域である複製領域67とを更に有する。

【0070】

尚、転送遅延部66は、本実施形態ではコントローラ63a内に実現されているよう記載しているが、コントローラ63b内に設けてもよいし、ポート65aと65bとの間に独立した装置として設けてもよい。また、本実施形態では記憶装置60a、60bはそれぞれ独立した装置として記載しているが、単一の記憶装置であってもよい。即ち、記憶領域64と複製領域67が同一記憶装置内に存在してもよい。更に、本実施形態では複製領域67は1個しか記載していないが、複数個存在してもよい。また、ポート65a、65bも、本実施形態では1個ずつしか記載していないが、それぞれ複数存在してもよい。

【0071】

データ保護装置 70 の構成は、第 1 の実施形態と同様である。しかし、プロセッサ 76 がデータ保護プログラム 74 を実行することにより仮想的に構成されるデータ保護部 74 x は、第 1 の実施形態における機能に加え、記憶領域 64 から複製領域 67 へのデータ反映を停止させる機能を更に保持する。

【0072】

本実施形態のシステムにおける動作は、基本的には第 1 の実施形態と同様である。しかし、記憶領域 64 の複製データを保持する複製領域 67 を予め設定し、更に転送遅延部 66 に記憶領域 64 から複製領域 67 へのデータ反映を ΔT 時間だけ遅らせるよう設定しておく点が、第 1 の実施形態とは異なる。これにより、通常運用時において複製領域 67 は常に記憶領域 64 の ΔT 時間前のデータを保持する。

【0073】

次に、本実施形態のシステムにおいてホスト 40 が不正行為を受けてから記憶領域 64 のデータを保護するまでの流れを説明する。データ保護部 74 x がホスト 40 と記憶領域 64 との間のバックエンドのパスを切断するような構成変更をスイッチ 50 あるいは SVP 62 a に対して命令するまでは、第 1 の実施形態と同様である。本実施形態ではこれに加え更に、データ保護部 74 x は、ポート 71 を介し、さらに、SVP 62 a または SVP 62 b を介し、コントローラ 63 a またはコントローラ 63 b に対し、記憶領域 64 と複製領域 67 との間の複製関係（データ反映）を解消あるいは一時停止するよう命令する。

【0074】

これにより、本実施形態では、第 1 の実施形態に加え更に、ホスト 40 に対する不正行為を検出した時刻より ΔT 時間前に記憶領域 64 が保持していたデータを複製領域 67 に確保できる。

【0075】

なお、ホスト 40 に対する不正行為を検出した時刻より ΔT 時間前に記憶領域 64 が保持していたデータを確保するという目的においては、記憶領域 64 と複製領域 67 との間の複製関係（データ反映）を解消あるいは一時停止すれば足り、ホスト 40 と記憶領域 64 との間のバックエンドのパスは、必ずしも切断しな

くてもよい。

【0076】

ここで、侵入検知部 4 3 x およびウイルス検知部 4 4 x が、不正行為がなされてから、最悪でも T_1 時間未満には不正行為を検出可能であるとする、 $\Delta T \geq T_1$ を満たすように ΔT を設定することにより、複製領域 6 7 に不正行為がなされる前のデータが格納されていることが保証される。このため、仮に記憶領域 6 4 のデータが被害を受けたとしても、複製領域 6 7 に格納したデータを用いることで、システムの早期復旧を図ることができる。

<第3の実施形態>

図 7 は、第 3 の実施形態のシステム構成を示したブロック図である。

【0077】

第 3 の実施形態のシステムは、フロントエンドのスイッチ 3 0 と、ホスト 4 0 と、バックエンドのスイッチ 5 0 と、記憶装置 6 0 と、データ保護装置 7 0 とを有し、ネットワーク 2 0 に接続している。また、ネットワークには計算機 1 0 が接続している。

【0078】

計算機 1 0 と、ネットワーク 2 0 と、フロントエンドのスイッチ 3 0 と、ホスト 4 0 と、バックエンドのスイッチ 5 0 とは、第 2 の実施形態と構成、機能とも同様とすることができる。

【0079】

記憶装置 6 0 は、第 1 の実施形態に加え、記憶領域 6 4 の複製データを保持する記憶領域である複製領域 6 7 a ~ 6 7 c を更に有する。尚、本実施形態では複製領域 6 7 a ~ 6 7 c を記憶領域 6 4 と同一の記憶装置 6 0 内部に設けるよう記載しているが、第 2 の実施形態と同様に異なる記憶装置に設けてもよい。また、複製領域は、本実施形態では 3 個記載しているが、複数であればいくつ存在してもよい。

【0080】

データ保護装置 7 0 の構成は、第 2 の実施形態と同様である。しかし、プロセッサ 7 6 がデータ保護プログラム 7 4 を実行することにより仮想的に構成される

データ保護部 74 x は、第 2 の実施形態における機能に加え、記憶領域 64 のデータを反映させる複製領域 67 a ~ 67 c を $\Delta T'$ 時間毎に順次切り替える機能を保持する。

【0081】

本実施形態のシステムにおける動作は、基本的には第 1 の実施形態と同様である。しかし、記憶領域 64 の複製データを保持する複製領域 67 a ~ 67 c を予め設定しておく点が第 1 の実施形態とは異なる。また、データ保護部 74 x が、 $\Delta T'$ 時間毎にポート 71、SVP 62 を介し、コントローラ 63 に対して、記憶領域 64 のデータを反映させる複製領域を切り替えるよう命令する点も異なる。

【0082】

図 8 は、本実施形態において記憶領域 64 のデータを反映させる複製領域 67 a ~ 67 c を切り替える流れを示したシーケンス図である。

【0083】

データ保護部 74 x は、ポート 71、SVP 62 を介し、コントローラ 63 に対して、記憶領域 64 のデータを複製領域 67 a に反映させるように命令する (S201)。次に、 $\Delta T'$ 時間経過後 (S202)、データ保護部 74 x は、ポート 71、SVP 62 を介し、コントローラ 63 に対して、記憶領域 64 と複製領域 67 a との間の複製関係を一時停止させ、記憶領域 64 のデータを複製領域 67 b に反映させるように命令する (S203)。更に、 $\Delta T'$ 時間経過後 (S204)、データ保護部 74 x は、ポート 71、SVP 62 を介し、コントローラ 63 に対して、記憶領域 64 と複製領域 67 b との間の複製関係を一時停止させ、記憶領域 64 のデータを複製領域 67 c に反映させるように命令する (S205)。

【0084】

そして、更に、 $\Delta T'$ 時間経過後 (S206)、データ保護部 74 x は、ポート 71、SVP 62 を介し、コントローラ 63 に対して、記憶領域 64 と複製領域 67 c との間の複製関係を一時停止させ (S207)、記憶領域 64 のデータを複製領域 67 a に反映させるように命令する (S201)。これらの処理を繰

り返すことにより、データ保護部 7 4 x は、記憶領域 6 4 のデータを反映させる複製領域 6 7 a ~ 6 7 c を、 $\Delta T'$ 時間毎に切り替える。なお、 $\Delta T'$ 時間毎に記憶領域 6 4 のデータを反映させる複製領域を切り替える処理は、コントローラ 6 3 が行なうようにしてもよい。

【0 0 8 5】

以上により、通常運用時において複製領域 6 7 a ~ 6 7 c は、それぞれ $\Delta T'$ 時間ずつずれた記憶領域 6 4 のスナップショットを保持する。

【0 0 8 6】

なお、記憶装置の中には、記憶領域 6 4 のデータを直接反映できる複製領域の数を制限し、前記各複製領域のデータを更に別の複数の複製領域に反映（多段接続）することにより、記憶領域 6 4 の複製を数多く保持できるものがある。

【0 0 8 7】

図 9 は、多段接続した場合の記憶領域と複製領域との関係の一例を示した図である。

【0 0 8 8】

複製領域 6 7 A は記憶領域 6 4 の複製先であるとともに、複製領域 6 7 A a、6 7 A b の複製元である。同様に、複製領域 6 7 B は記憶領域 6 4 の複製先であるとともに、複製領域 6 7 B a、6 7 B b の複製元である。

【0 0 8 9】

このような記憶装置に対しては、データ保護部 7 4 x は、例えば、まず、ポート 7 1、SVP 6 2 を介し、コントローラ 6 3 に対して、記憶領域 6 4 のデータを複製領域 6 7 A に反映させ、複製領域 6 7 A のデータを複製領域 6 7 A a に反映させるよう命令する。次に、 $\Delta T'$ 時間経過後、データ保護部 7 4 x は、ポート 7 1、SVP 6 2 を介し、コントローラ 6 3 に対して、複製領域 6 7 A と複製領域 6 7 A a との間の複製関係を一時停止させ、複製領域 6 7 A のデータを複製領域 6 7 A b に反映させるよう命令する。更に、 $\Delta T'$ 時間経過後、データ保護部 7 4 x は、ポート 7 1、SVP 6 2 を介し、コントローラ 6 3 に対して、複製領域 6 7 A と複製領域 6 7 A b、及び記憶領域 6 4 と複製領域 6 7 A との間の複製関係を一時停止させ、記憶領域 6 4 のデータを複製領域 6 7 B に反映させ、複

製領域 6 7 B のデータを複製領域 6 7 B b に反映させるよう命令する。更に、 $\Delta T'$ 時間経過後、データ保護部 7 4 x は、ポート 7 1、SVP 6 2 を介し、コントローラ 6 3 に対して、複製領域 6 7 B と複製領域 6 7 B a との間の複製関係を一時停止させ、複製領域 6 7 B のデータを複製領域 6 7 B b に反映させるよう命令する。これを繰り返すことにより、データ保護部 7 4 x は、別の複製領域に対する複製元でない末端の複製領域 6 7 A a、6 7 A b、6 7 B a、6 7 B b に対し、記憶領域 6 4 の $\Delta T'$ 時間毎のスナップショットを保持させることができる。

【0 0 9 0】

本実施形態のシステムにおいてホスト 4 0 が不正行為を受けてから記憶領域 6 4 のデータを保護するまでの流れは第 2 の実施形態と同様である。ただし、すべての複製領域 6 7 との間の複製関係を停止させる。

【0 0 9 1】

以上より、本実施形態には第 1 の実施形態に加え更に、N 個の複製領域に記憶領域 6 4 の $\Delta T'$ 時間毎のスナップショットを保持する効果がある。図 7 の例では N は 3 としている。

【0 0 9 2】

なお、ホスト 4 0 に対する不正行為がなされる前のデータを確保するという目的においては、記憶領域 6 4 とすべての複製領域 6 7 との間の複製関係（データ反映）を解消あるいは一時停止すれば足り、ホスト 4 0 と記憶領域 6 4 との間のバックエンドのパスは、必ずしも切断しなくてもよい。

【0 0 9 3】

ここで、侵入検知部 4 3 x およびウイルス検知部 4 4 x が、不正行為がなされてから、最悪でも T_1 時間未満には不正行為を検出可能であるとする、 $\Delta T' \geq T_1 / (N - 2)$ を満たすように $\Delta T'$ を設定することにより、少なくとも 1 個の複製領域 6 7 には不正行為がなされる前のデータが格納されていることが保証される。なぜなら、記憶領域 6 4 のデータを反映させる複製領域を切り替えた直後に不正行為が検出されるという最悪のケースであっても、N 個の複製領域 6 7 のそれぞれには、記憶領域 6 4 の 0 時間前（現在の複製対象）、0 時間前（直

前の複製対象)、 $\Delta T'$ 時間前、…、 $(N-2) \Delta T'$ 時間前のデータが保持されているからである。すなわち、 $\Delta T' \geq T1 / (N-2)$ であれば、 $(N-2) \Delta T'$ 時間前のデータは、 $T1$ 時間前のデータより以前のものであり、不正行為が行われたのは $T1$ 時間前より以降である。このため、 N 個の複製領域 6 7 のうち 1 個は記憶領域 6 4 の $(N-2) \Delta T'$ 時間前の、不正行為が行われる以前のデータを保持していることになる。これにより、仮に記憶領域 6 4 のデータが被害を受けたとしても、いずれかの複製領域 6 7 に格納したデータを用いることで、システムの早期復旧を図ることができる。

【0 0 9 4】

また、不正行為検出後にログファイルの解析などを行うことによって、記憶領域 6 4 のデータが破壊され始めた時刻、あるいは不正行為が開始された時刻が具体的に判明することがある。本実施形態では、前記時刻より以前のうちの最新である $T1 / (N-2)$ 時間前のデータを確保可能である。この点において、少なくとも $T1$ 時間分のデータロスが発生する第 2 の実施形態に比して有利である。

【0 0 9 5】

さらに、本実施形態においてログデータを記憶領域 6 4 に格納するようにすると、不正行為の検出にも役立つ。クラッカー（侵入者）は不正アクセスの痕跡を消すためにログを改竄することがある。本実施形態ではログデータの $\Delta T'$ 時間毎のスナップショットを複製領域 6 7 に保持できる。例えば、ログ改竄検出プログラムをデータ保護装置 7 0、ホスト 4 0、他の計算機、またはコントローラ 6 3 等に格納し、このプログラムを実行することにより各複製領域に格納されたログデータを比較することによりログの改竄を検出するログ改竄検出部を仮想的に構成することで、ホスト 4 0 に対する不正行為の監視を行なうことができる。すなわち、ログ改竄検出部がログの改竄を検出すると、不正行為受信プログラム 7 3 に通知するようにすれば、ホスト 4 0 が使用する記憶領域のデータを保護できる。また、複製領域に格納されたログデータのスナップショットを解析することで、再侵入を企てようとするクラッカーを特定したり、待ち受け等の対策を行なうことが可能となる。

【0 0 9 6】

【発明の効果】

上述のように、本発明によれば、計算機システムに対する不正行為を検出した場合に、計算機システムのデータを保護することができる。

【図面の簡単な説明】

【図 1】 第 1 の実施形態のシステム構成を示すブロック図である。

【図 2】 第 1 の実施形態における、不正行為がホスト 4 0 になされてから記憶領域 6 4 のデータを保護するまでの処理の流れを表すシーケンス図である。

【図 3】 第 1 の実施形態におけるスイッチ 5 0 が保持するゾーニングテーブル 1 0 0 の一例を表す図である。

【図 4】 第 1 の実施形態におけるコントローラ 6 3 が保持するパス構成テーブル 1 1 0 の一例を表す図である。

【図 5】 第 1 の実施形態におけるコントローラ 6 3 が保持する A C L テーブル 1 2 0 の一例を表す図である。

【図 6】 第 2 の実施形態におけるシステム構成を示すブロック図である。

【図 7】 第 3 の実施形態におけるシステム構成を示すブロック図である。

【図 8】 第 3 の実施形態における、記憶領域 6 4 の複製対象となる複製領域 6 7 a ~ 6 7 c を切り替える処理の流れを表すシーケンス図である。

【図 9】 第 3 の実施形態における複製領域の多段接続の一例を表す図である。

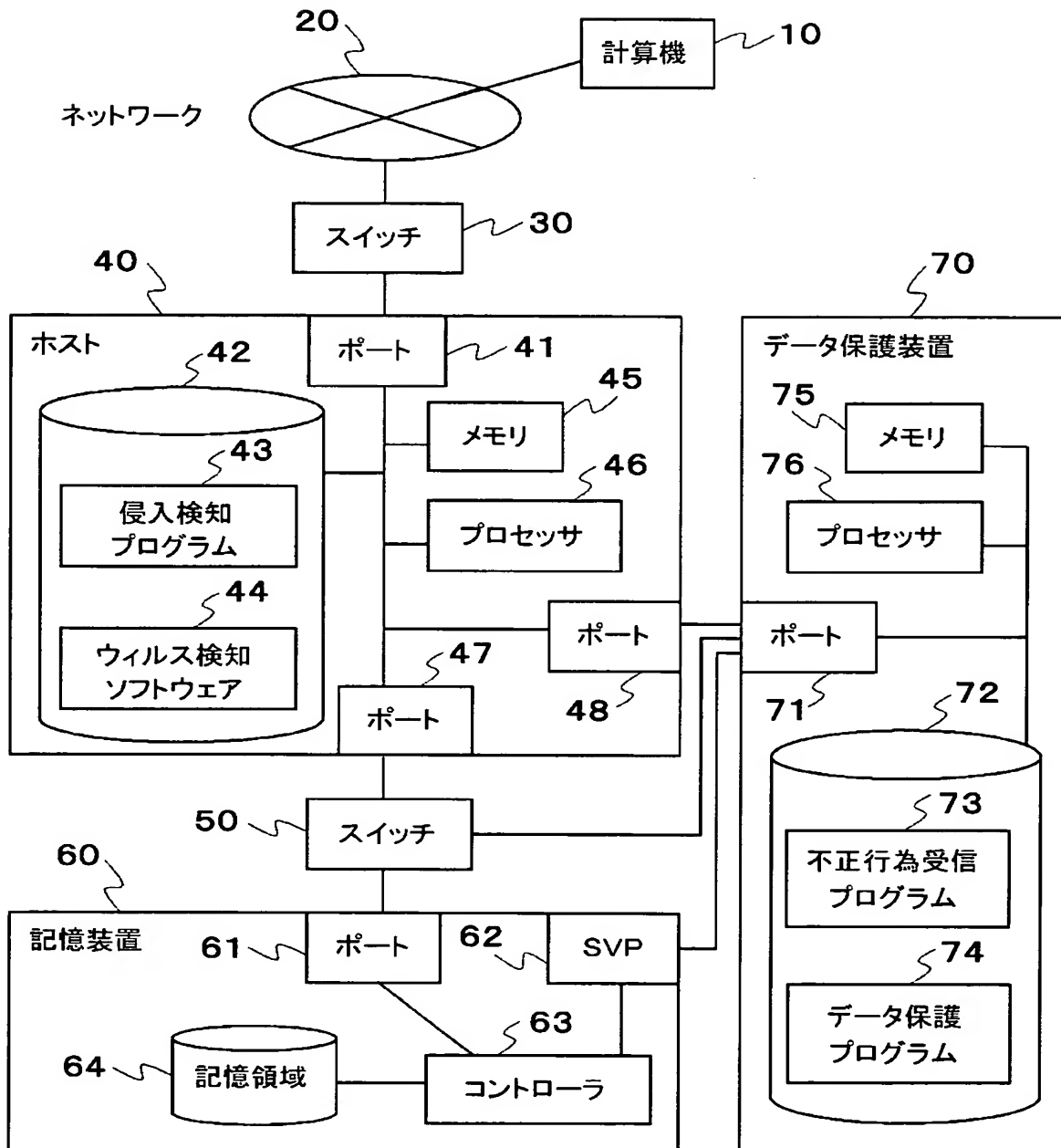
【符号の説明】

1 0 … 計算機、2 0 … ネットワーク、3 0 … (フロントエンド) スイッチ、4 0 … ホスト、4 3 … 侵入検知プログラム、4 4 … ウィルス検知ソフトウェア、5 0 … (バックエンド) スイッチ、6 0 … 記憶装置、6 2 … S V P、6 3 … コントローラ、6 4 … 記憶領域、6 6 … 転送遅延部、6 7 … 複製領域、7 0 … データ保護装置、7 3 … 不正行為受信プログラム、7 4 … データ保護プログラム、1 0 0 … ゾーニングテーブル、1 1 0 … パス構成テーブル、1 2 0 … A C L テーブル

【書類名】 図面

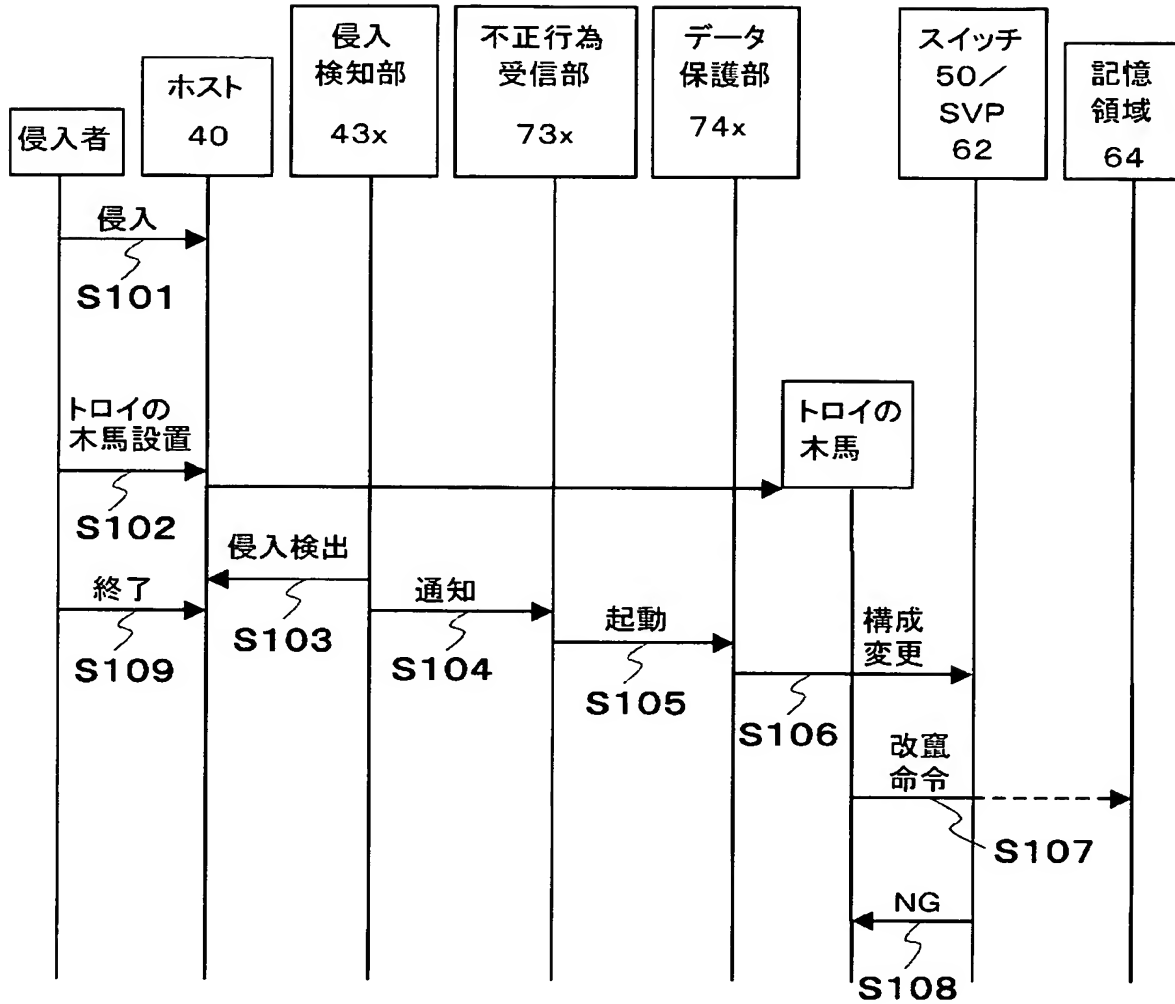
【図 1】

図 1



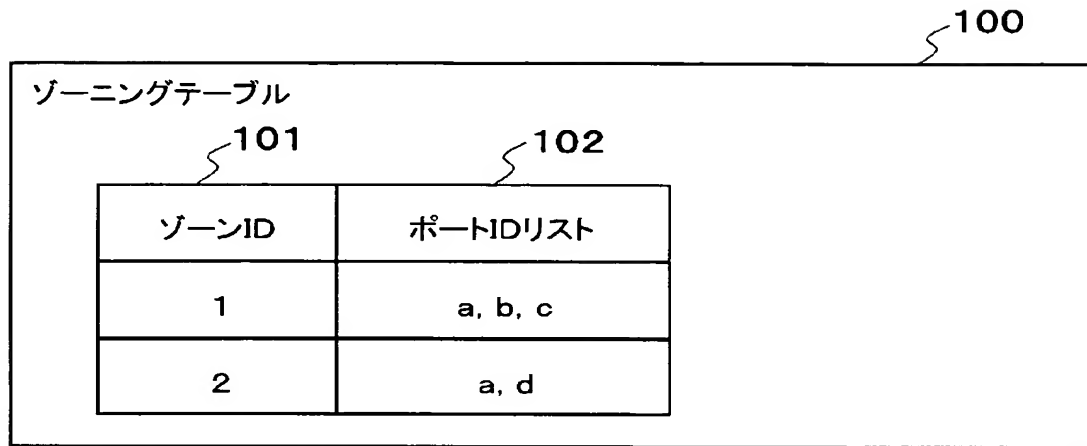
【図 2】

図2



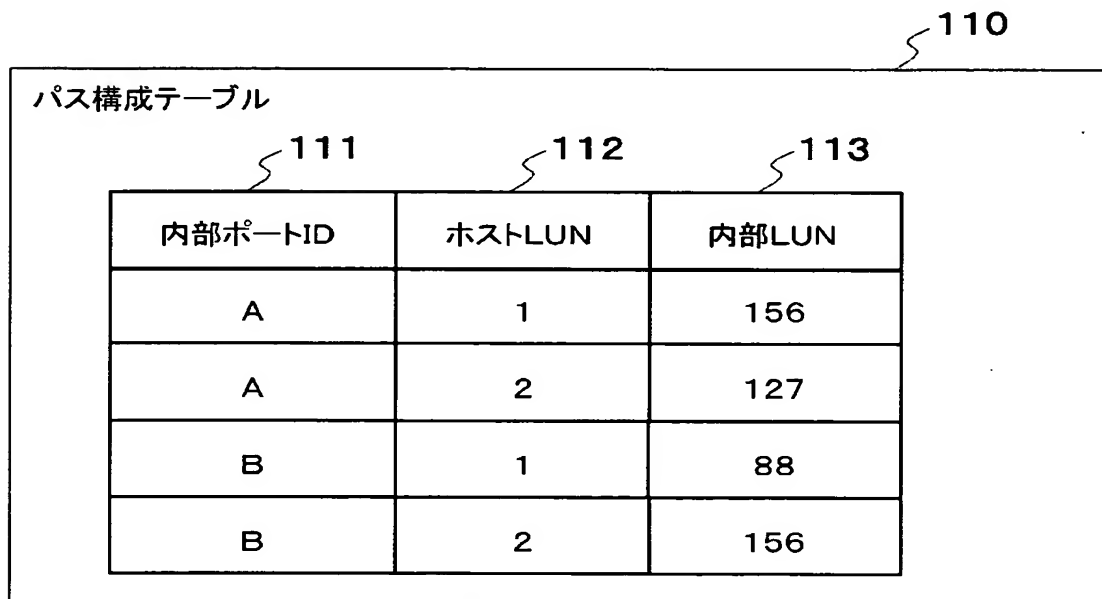
【図 3】

図 3



【図 4】

図 4



【図 5】

図5

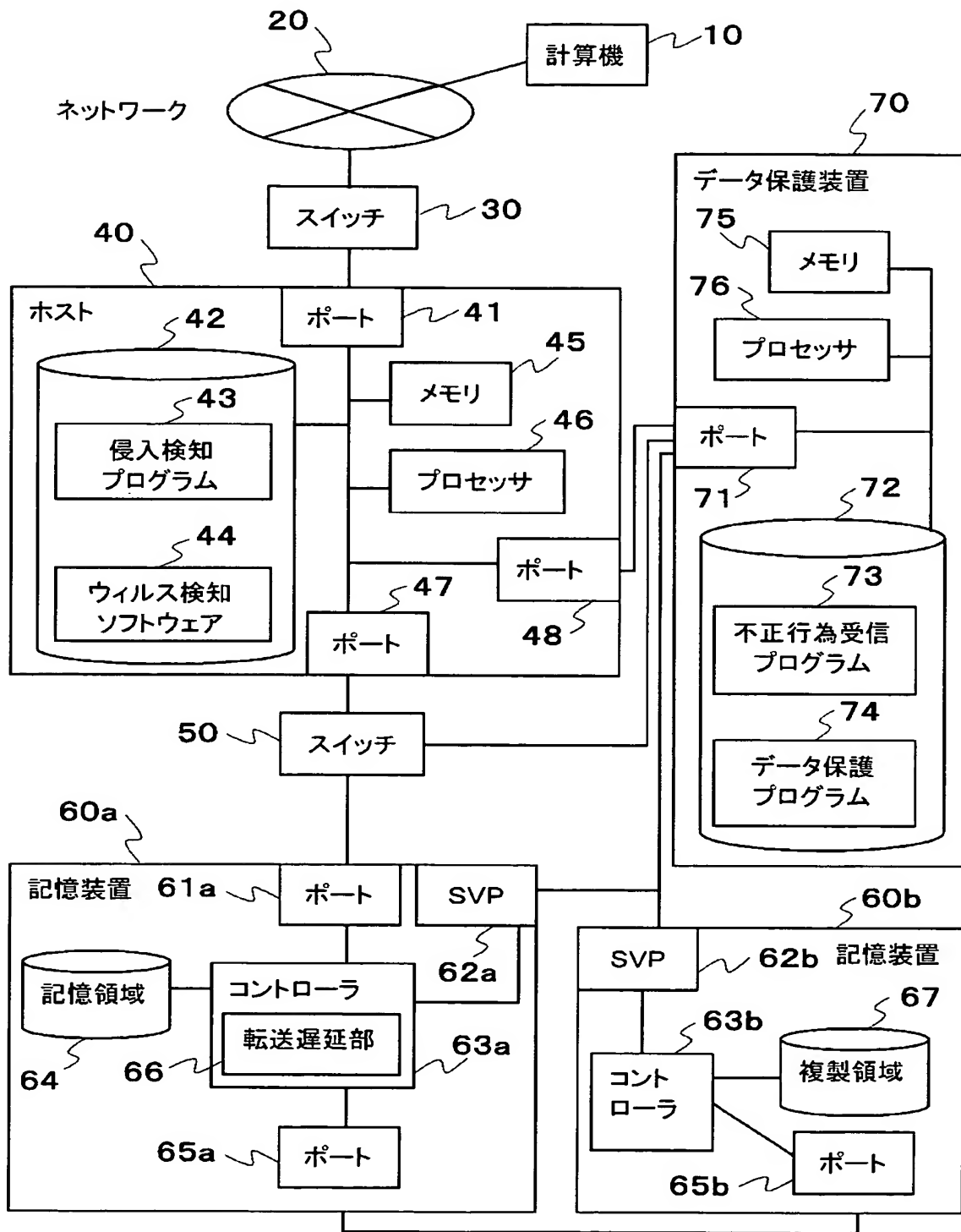
120

ACLテーブル

121	122	123
内部ポートID	ホストLUN	ホストポートIDリスト
A	1	a, b, c
A	2	a, d, e
B	1	d, e
B	2	b, c

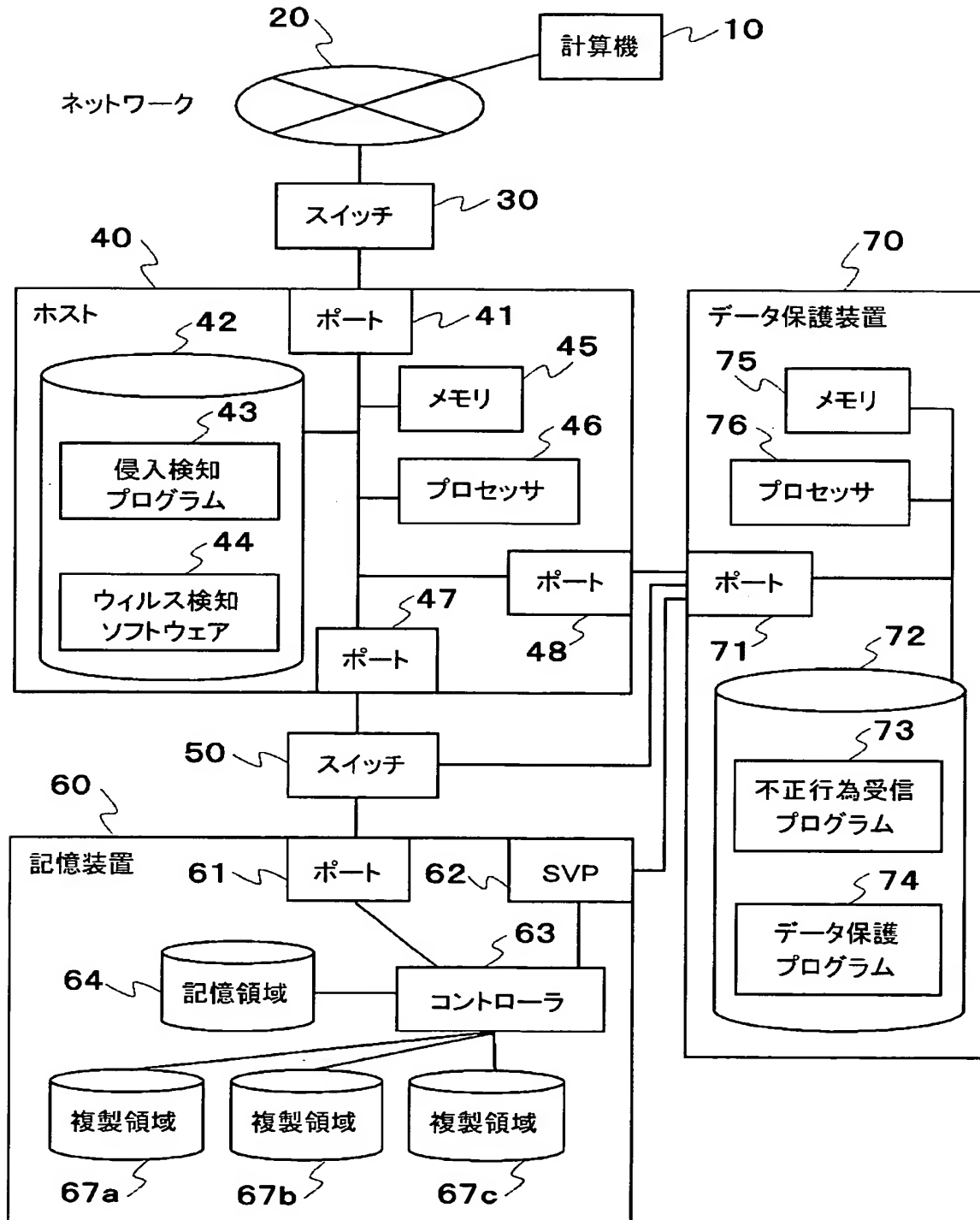
【図 6】

図6



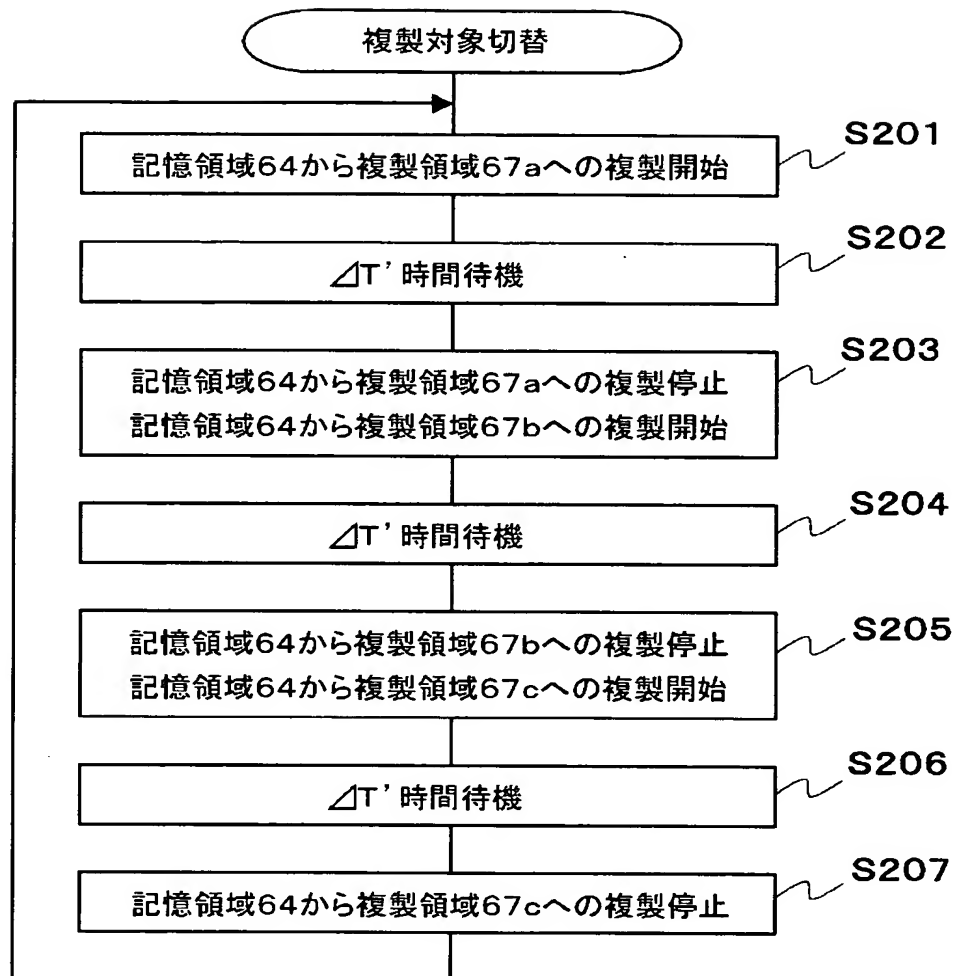
【図 7】

図 7



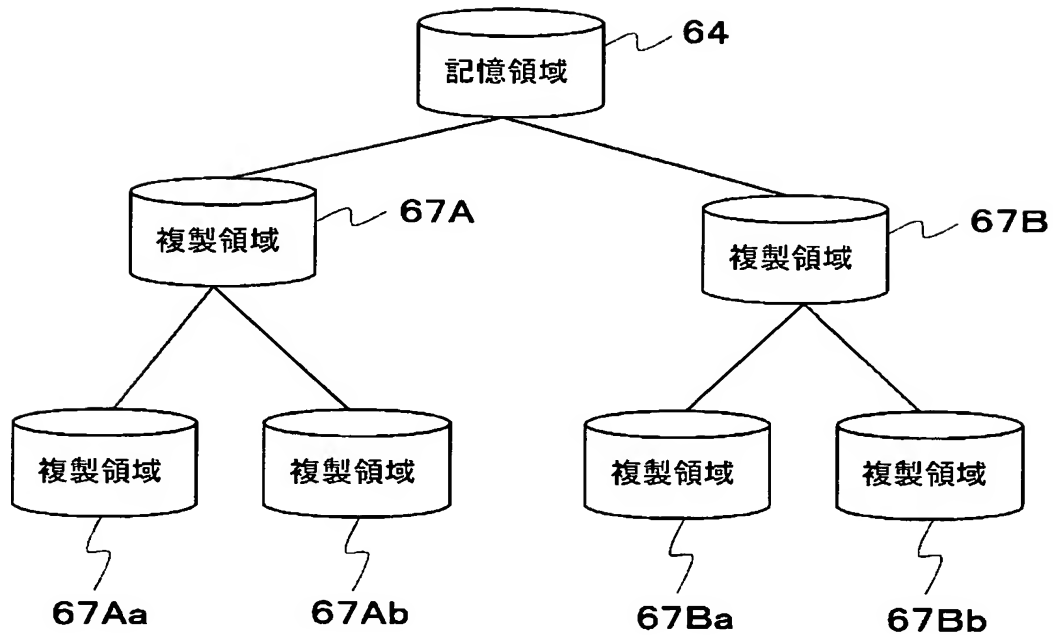
【図 8】

図 8



【図 9】

図9



【書類名】 要約書

【要約】

【課題】 計算機システムに対する不正行為を検出した場合に、計算機システムのデータを保護する。

【解決手段】 データを記憶するために割り当てられる記憶領域と、前記記憶領域に対してデータの読み込みまたは書き込みを行う計算機と、前記計算機と前記記憶領域との通信を制御する記憶制御装置とを有する計算機システムに対して、前記記憶領域のデータを保護するデータ保護装置であって、イベントの発生を検出するイベント検出部と、前記イベント検出部がイベントを検出すると、前記計算機と前記記憶領域との通信を停止するよう前記記憶制御装置に対して指示するパス切断部とを有するデータ保護装置。

【選択図】 図 1

特願 2 0 0 3 - 1 5 4 8 7 0

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所